

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-057662

(43)Date of publication of application : 22.02.2002

(51)Int.Cl.

H04L 9/10
H04L 9/14

(21)Application number : 2000-238815

(71)Applicant : SONY CORP

(22)Date of filing : 07.08.2000

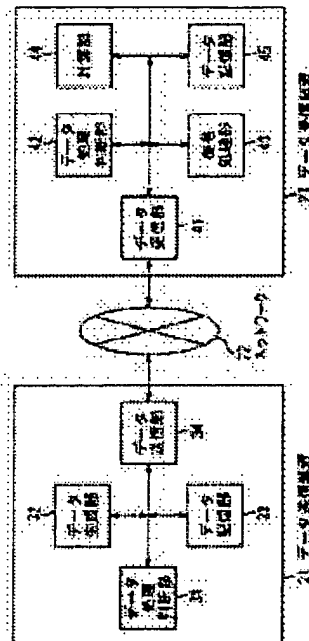
(72)Inventor : MUTO AKIHIRO

(54) INFORMATION-PROCESSING DEVICE AND METHOD, AND RECORD MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To secure a processing capacity for decoding coded contents data.

SOLUTION: A data reception device 23 for receiving contents data transmitted from a data transmission device 21 for decoding processing confirms the details of meta data where information regarding the coding of the contents data is described. When a plurality of data processings are requested by a decoding processing part 43, the decoding processing part 43 selects top priority processing from each processing order being set to the meta data, and performs processing from the top priority processing. The decoding processing part 43 calculates time required for other processing, and judges whether other processing can be made or not until the data unit of the contents data requiring the next top priority processing is transmitted from a data processing judgment part 42. The decoding processing part 43 performs processing when it judges that other processing can be made, and confirms the handling information of other processing being set to the meta data when other processing cannot be made, and performs processing based on the handling information.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-57662

(P2002-57662A)

(43) 公開日 平成14年2月22日 (2002.2.22)

(51) Int.Cl.	識別記号	FI	キーワード (参考)
H04L 9/10		H04L 9/00	621Z 5J104
9/14			641

審査請求 未請求 請求項の数 4 OL (全 26 頁)

(21) 出願番号 特願2000-238815 (P2000-238815)

(22) 出願日 平成12年8月7日 (2000.8.7)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 武藤 明宏

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム (参考) 5J104 AA01 AA32 DA04 JA13 JA28

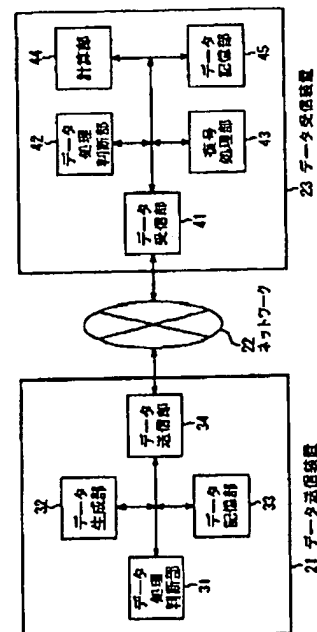
PA07 PA10

(54) 【発明の名称】 情報処理装置、情報処理方法、並びに記録媒体

(57) 【要約】

【課題】 暗号化されたコンテンツデータを復号する処理能力を確保する。

【解決手段】 データ送信装置21から送信されるコンテンツデータを受信して復号処理するデータ受信装置23は、コンテンツデータを処理する前に、コンテンツデータの暗号化に関する情報が記述されているメタデータの内容を確認する。複数のデータ処理が復号処理部43に要求されている場合、復号処理部43は、メタデータにより設定されているそれぞれの処理順位から、最優先処理を選択し、最優先処理から処理を行う。復号処理部43は、他の処理に要する時間を算出し、次の最優先処理に必要なコンテンツデータのデータ単位が、データ処理判断部42から転送されてくるまでの間に、他の処理を行うことが可能であるか否かを判定する。復号処理部43は、他の処理を行うことが可能と判定した場合、処理を行い、不可能と判定した場合、メタデータに設定されている他の処理の取扱情報を確認し、取扱情報に基づいて処理する。



【特許請求の範囲】

【請求項1】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、前記受信手段により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識手段と、

前記第1の認識手段により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータの他の処理に優先して処理する第1の処理手段とを含むことを特徴とする情報処理装置。

【請求項2】 前記他の処理に要する時間を算出する算出手段と、

第1の前記優先処理に必要な前記コンテンツデータの処理が終了されている場合、第2の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間と、前記算出手段により算出された前記他の処理に要する時間を比較する比較手段と、

前記比較手段による比較の結果、前記第2の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間が、前記他の処理に要する時間より長いと判定された場合、前記他の処理を処理する第2の処理手段と、

前記比較手段による比較の結果、前記第2の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間が、前記他の処理に要する時間より短いと判定された場合、前記他の処理の取扱方法を認識する第2の認識手段と、

前記第2の認識手段により認識された取扱方法に基づいて前記他の処理を処理する第3の処理手段とをさらに含むことを特徴とする請求項1に記載の情報処理装置。

【請求項3】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識ステップと、

前記第1の認識ステップの処理により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータの他の処理に優先して処理する第1の処理ステップとを含むことを特徴とする情報処理方法。

【請求項4】 コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識ステップと、

前記第1の認識ステップの処理により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータ

の他の処理に優先して処理する第1の処理ステップとを含むことを特徴とするコンピュータが読みとり可能なプログラムが格納されている記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および情報処理方法、並びに記録媒体に関し、特に、要求されるデータ処理毎に設定されている処理順位を認識し、処理順位が上位にあるデータ処理を優先的に処理することにより、システム毎に設計したハードウェアを用いることなく、迅速にデータを処理することができるようにした情報処理装置および情報処理方法、並びに記録媒体に関する。

【0002】

【従来の技術】近年、コンテンツデータをネットワークを介して配信する配信システムが構築されている。配信されるコンテンツデータは、データの改竄を防ぐため、暗号化や、デジタル署名を付加するなどの処理が施されている。暗号化されたコンテンツデータは、利用者の端末により復号処理され、利用者はそれを利用することができる。

【0003】暗号化技術の安全性は、復号する際の処理の難しさに依存しているため、暗号化技術の高度化にともなって、コンテンツデータを利用する利用者の端末には、より処理能力の高い端末が要求されるようになっていく。

【0004】そこで、処理能力を確保するために、利用者端末に復号処理専用のLSI (Large Scale Integration) を配置することが考えられる。図1は、復号処理専用のLSI (以下、復号LSIと称する) の構成例を示している。

【0005】復号LSI 1は、復号LSI 1の外部に配置されるコントロールマイクロコンピュータ (以下、コントロールマイコンと略称する) 2から転送される指令により復号処理を行う。復号処理には、暗号化されたコンテンツデータを復号する処理の他に、コンテンツデータに付加されているデジタル署名を検証する処理が含まれる。復号LSI 1が処理した結果は、復号LSI 1の外部に配置される外部メモリ3に記憶される。

【0006】復号LSI 1は、通信インタフェース11、コントロールユニット12、RAM (Random Access Memory) 13、メモリコントローラ14、フラッシュメモリ15、べき乗演算器16、ハッシュ値演算器17から構成される。

【0007】コントロールマイコン2から転送される指令は、通信インタフェース11を介してコントロールユニット12に伝えられる。コントロールユニット12は、べき乗演算器16およびハッシュ値演算器17などを補助的に用いつつ、復号LSI 1の全体の動作を制御し、暗号化されているデータの復号処理、およびディジ

タル署名の検証処理などを行う。

【0008】RAM 13には、コントロールユニット12が利用するプログラムが記憶されている。

【0009】メモリコントローラ14は、外部メモリ3に対するデータの読み書きを制御する。

【0010】フラッシュメモリ15には、コントロールユニット12の指令によりべき乗演算器16、およびハッシュ値演算器17が演算した結果や、処理に必要なデータが、適宜、記憶される。

【0011】利用者が使用する端末に、上述したような復号LSI 1を配置することにより、コンテンツデータの復号処理能力を確保することが可能となる。

【0012】

【発明が解決しようとする課題】しかしながら、利用者端末に復号LSI 1（ハードウェア）を設置する場合、暗号化されたコンテンツデータの復号処理能力は、暗号化のセキュリティレベルに応じて計算量が異なるため、最大の負荷を処理することができるように復号LSI 1を構成する必要がある。その結果、コスト高となる課題があった。また、処理能力を変更する必要がある場合、LSIを設計し直す必要があるため、バージョンアップ等の変更が実質的に困難になる課題があった。

【0013】本発明はこのような状況に鑑みてなされたものであり、暗号化されたコンテンツデータを利用者端末において復号する場合に、システム毎に設計したハードウェアを利用することなく、低コストで、かつ、比較的容易に機能を変更できるシステムを実現できるようにするものである。

【0014】

【課題を解決するための手段】本発明の情報処理装置は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、受信手段により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識手段と、第1の認識手段により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第1の処理手段とを含むことを特徴とする。

【0015】本発明の情報処理装置は、他の処理に要する時間を算出する算出手段と、第1の優先処理が必要なコンテンツデータの処理が終了されている場合、第2の優先処理が必要なコンテンツデータの処理が開始されるまでの時間と、算出手段により算出された他の処理に要する時間を比較する比較手段と、比較手段による比較の結果、第2の優先処理が必要なコンテンツデータの処理が開始されるまでの時間が、他の処理に要する時間より長いと判定された場合、他の処理を処理する第2の処理手段と、比較手段による比較の結果、第2の優先処理が必要なコンテンツデータの処理が開始されるまでの時間が、他の処理に要する時間より短いと判定された場合、

他の処理の取扱方法を認識する第2の認識手段と、第2の認識手段により認識された取扱方法に基づいて他の処理を処理する第3の処理手段とをさらに含むようにすることができる。

【0016】本発明の情報処理方法は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識ステップと、第1の認識ステップの処理により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第1の処理ステップとを含むことを特徴とする。

【0017】本発明の記録媒体のプログラムは、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第1の認識ステップと、第1の認識ステップの処理により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第1の処理ステップとを含むことを特徴とする。

【0018】本発明の情報処理装置、情報処理方法、および記録媒体においては、コンテンツデータと、その特徴に関する情報が記述されている特徴情報が受信され、受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位が認識される。処理順位が上位にある優先処理は、コンテンツデータの他の処理に優先して処理される。

【0019】

【発明の実施の形態】図2は、本発明を適用したデータ処理システムの構成例を示すブロック図である。データ送信装置21により生成され、暗号化されたコンテンツデータは、ネットワーク22を介してデータ受信装置23に送信される。

【0020】データ送信装置21は、データ処理判断部31、データ生成部32、データ記憶部33、およびデータ送信部34から構成される。

【0021】データ処理判断部31は、データ送信装置21の全体の動作を制御する。データ生成部32は、所定の方法により提供されたコンテンツデータを暗号化したり、デジタル署名を生成する（以下、コンテンツデータの暗号化処理、およびデジタル署名の生成処理をまとめて暗号関連処理と称する）。また、データ生成部32は、コンテンツデータの暗号化に関するデータなどが記述されているメタデータを生成する。データ記憶部33は、データ生成部32により生成されたコンテンツデータおよびメタデータを記憶する。データ送信部34は、データ受信装置23からの要求に応じて、データ記憶部33に記憶されているメタデータおよびコンテンツ

データを送信する。

【0022】ネットワーク22は、データ送信装置21およびデータ受信装置23の間で送受信されるデータの伝送路であり、例えば、インターネット、電話回線網、ケーブルテレビジョン放送網、衛星を介したデジタルテレビジョン放送網等により構成される。

【0023】データ受信装置23は、データ受信部41、データ処理判断部42、復号処理部43、計算部44、およびデータ記憶部45より構成される。

【0024】データ受信部41は、データ送信装置21から送信されたメタデータおよびコンテンツデータを受信する。データ処理判断部42は、データ受信装置23の全体の動作を制御する。復号処理部43は、データ受信部41により受信されたコンテンツデータが暗号化されている場合にはコンテンツデータを復号し、デジタル署名が付加されている場合には、デジタル署名の検証などの処理を行う（以下、コンテンツデータの復号処理、およびデジタル署名の検証処理をまとめて復号関連処理と称する）。計算部44は、データ処理判断部42の指令を受けて、演算処理機能を提供する。データ記憶部45は、データ受信部41により受信されたコンテンツデータ、および復号処理部43により復号され、かつデジタル署名が検証されたコンテンツデータを記憶する。

【0025】次に、データ送信装置21が送信するメタデータおよびコンテンツデータを、データ受信装置23が受信し、処理する一連の処理について、図3乃至図5のフローチャートを参照して説明する。

【0026】図3は、データ送信装置21の処理を説明するフローチャートである。ステップS1において、データ生成部32は、外部から所定の方法により提供されるアナログデータまたはデジタルデータを取得し、コンテンツデータを作成する。データ生成部32は、ネットワーク22を介してデータ受信装置23に対して送信することが可能な形式に圧縮し、暗号関連処理を施して、コンテンツデータを作成する。

【0027】また、データ生成部32は、メタデータを生成する。メタデータには、送信されるコンテンツデータの特徴、コンテンツデータの暗号関連処理に関する情報である暗号関連情報、およびデータ受信装置23がコンテンツデータを処理するために必要な情報が記述される。コンテンツデータの特徴には、例えば、コンテンツデータの制作者、制作時期、制作者を識別する制作者ID、コンテンツデータの利用形態、コンテンツデータ利用形態毎の料金、コンテンツデータの再生時間、コンテンツデータの圧縮方法、総データ量、データの転送速度などが含まれる。また、コンテンツデータの暗号関連情報には、例えば、暗号化アルゴリズム、デジタル署名の生成アルゴリズム、データ単位が含まれる。さらに、データ受信装置23がコンテンツデータを処理するため

に必要な情報には、コンテンツデータの処理の種類、コンテンツデータの転送周期、処理順位、および取扱情報が含まれる。これらの具体例については後述する。

【0028】ステップS2において、データ記憶部33は、ステップS1の処理でデータ生成部32により作成されたコンテンツデータおよびメタデータを記憶する。

【0029】ステップS3において、データ処理判断部31は、データ受信装置23からメタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。データ処理判断部31によりメタデータの送信が要求されたと判定された場合、処理はステップS4に進む。

【0030】ステップS4において、データ送信部34は、データ記憶部33に記憶されているメタデータを、ネットワーク22を介してデータ受信装置23に送信する。後述するように、メタデータを受信したデータ受信装置23は、メタデータに記述されている情報を分析し、コンテンツデータの処理を準備する。メタデータに記述されているコンテンツデータの情報に応じて、コンテンツデータを処理する準備が完了した場合、データ受信装置23は、コンテンツデータの送信をデータ送信装置21に要求する。

【0031】そこで、ステップS5において、データ処理判断部31は、データ受信装置23からコンテンツデータの送信が要求されたか否かを判定する。

【0032】ステップS5において、データ処理判断部31によりデータ受信装置23からコンテンツデータの送信が要求されていないと判定された場合、データ処理判断部31は、データ受信装置23が、コンテンツデータの処理の準備が完了していないと認識し、コンテンツデータの送信が要求されるまで待機する。

【0033】ステップS5において、データ処理判断部31が、データ受信装置23からコンテンツデータの送信が要求されたと判定した場合、処理はステップS6に進み、データ送信部34は、データ記憶部33に記憶されているコンテンツデータを、ネットワーク22を介してデータ受信装置23に対して送信する。

【0034】図4および図5は、データ受信装置23の処理を説明するフローチャートである。ステップS11において、データ処理判断部42は、データ受信装置23を管理する利用者からコンテンツデータの受信の指令が入力された場合、データ送信装置21に対して、そのコンテンツデータに対応するメタデータの送信を要求する。

【0035】ステップS12において、データ受信部41は、データ送信装置21から送信されたメタデータを、ネットワーク22を介して受信する。データ受信部41が受信したメタデータは、データ処理判断部42に転送され、データ処理判断部42により記述されている内容が分析される。データ処理判断部42は、コンテン

ツデータは暗号関連処理が施されていると認識し、メタデータを復号処理部43に転送する。

【0036】ステップS13において、復号処理部43は、メタデータに記述されている内容を分析し、全ての復号関連処理を抽出する。

【0037】ステップS14において、復号処理部43は、メタデータを参照して、ステップS13で抽出された復号関連処理から、データ処理判断部42が復号処理部43に対して処理を要求するタイミング（データ処理部42が復号処理部43に対してコンテンツデータを転送するタイミング）に周期性がある処理をさらに抽出する。

【0038】ステップS15において、ステップS14の処理で抽出した処理から、メタデータに予め設定されているそれぞれの処理の優先度を示す処理順位を確認し、処理順位が最上位にある復号関連処理を最優先処理として選択する。

【0039】ステップS16において、復号処理部43は、最優先処理が必要なコンテンツデータの転送周期を基準周期として設定する。

【0040】ステップS17において、復号処理部43から、最優先処理を選択し、基準周期を設定した旨の通知を受けたデータ処理判断部42は、データ送信装置21に対してコンテンツデータの送信を要求する。

【0041】ステップS18において、データ受信部41は、データ送信装置21が送信したコンテンツデータを、ネットワーク22を介して受信する。

【0042】データ受信装置41からコンテンツデータを受け取ったデータ処理判断部42は、復号関連処理が必要なコンテンツデータ単位を復号処理部43に転送する前に、ステップS19の判定処理を行う。ステップS19において、データ処理判断部42は、復号関連処理が必要なコンテンツデータの処理が終了したか否かを判定する。処理開始時においては、復号関連処理が必要なコンテンツデータがまだ存在しているため、処理は終了することができないと判定され、ステップS20に進む。

【0043】ステップS20において、データ処理判断部42は、復号処理部43に対して復号関連処理が必要なコンテンツデータ単位を転送する。転送されるコンテンツデータ単位は、ステップS16で設定した基準周期に基づいて、最優先処理が必要なコンテンツデータ単位から転送される。復号処理部43により復号関連処理が施されたコンテンツデータ単位は、データ記憶部45に、適宜、記憶される。以下、図6を参照してデータ処理判断部42が転送するコンテンツデータ単位について説明する。

【0044】最優先処理データ単位1がデータ処理判断部42から転送される時間を時間0として、ステップS16の処理で設定した基準周期毎に最優先処理データ単位が転送される。図6では、基準周期毎に最優先処理デ

ータ単位2、最優先処理データ単位3、および最優先処理が必要なコンテンツデータ単位の最後のコンテンツデータ単位である最優先処理データ単位nが転送されている。また、最優先処理データ単位nの後には後述する遅延処理データが転送されている。

【0045】タイム1、およびタイム2は基準周期の時間の長さを示しており、タイム1、およびタイム2はそれぞれ、タイム1-1、タイム2-1、およびタイム1-2、タイム2-2に分かれている。

【0046】タイム1-1、タイム2-1、タイムn-1はそれぞれ最優先処理データ単位1、最優先処理データ単位2、および最優先処理データ単位nを、復号処理部43が復号関連処理する際に要する時間である。

【0047】タイム1-2、タイム2-2はそれぞれ復号処理部43が最優先処理データ単位1、または最優先処理データ単位2の復号関連処理を終了し、次のコンテンツデータ単位が転送されるのを待機している時間である。本発明では、タイム1-2、タイム2-2において、復号処理部43は、最優先処理以外の他の復号関連処理が実行可能であるか否かを判断するが、その処理については後述する。

【0048】ステップS21において、復号処理部43は、データ処理判断部42から転送された最優先処理が必要なコンテンツデータ単位の処理を行う。すなわち、復号処理部43は、最優先処理データ単位1を受信した場合、処理を開始する。

【0049】ステップS22において、復号処理部43は、最優先処理以外の復号関連処理が必要なコンテンツデータ単位（以下、単に、他のコンテンツデータ単位と称する）が、データ処理判断部42から転送されてきたか否かを判定する。復号処理部43が、他のコンテンツデータ単位が転送されてきたと判定するまでステップS19乃至ステップS21の処理は繰り返される。

【0050】ステップS22において、復号処理部43は、他のコンテンツデータ単位がデータ処理判断部42から転送されてきたと判定した場合、処理はステップS23に進む。

【0051】ステップS23において、復号処理部43は、図6の最優先処理データ単位1の処理を終了しており、最優先処理データ単位2がデータ処理判断部42から転送されてくるのを待機している状態の場合（タイム1-2の状態の場合）、データ処理判断部42から転送されてきた他のコンテンツデータ単位の復号関連処理に要する時間を算出する。データ処理判断部42から転送されてきた他のコンテンツデータ単位が複数ある場合、復号処理部43は、ステップS15で認識した復号関連処理の処理順位を確認し、転送されてきているコンテンツデータ単位に必要な復号関連処理のうちの最も処理順位が高い処理に要する時間を算出する。なお、復号処理部43は、最優先処理を実行している場合（タイム1-

1の状態の場合)、データ処理判断部42から転送されてくる他のコンテンツデータ単位を無視して最優先処理を続行する。

【0052】ステップS24において、復号処理部43は、ステップS23で算出した他のコンテンツデータ単位の処理に要する時間から、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理が可能かを判定する。すなわち、復号処理部43は、タイム1-2の間に、他のコンテンツデータ単位の処理を完了することが可能かを判定する。

【0053】ステップS24において、復号処理部43は、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理を完了することは可能と判定した場合、処理はステップS25に進み、復号処理部43は、他のコンテンツデータ単位の復号関連処理を行う。その後、処理はステップS22の処理に戻り、以降の処理が繰り返し実行される(復号関連処理が必要なコンテンツデータが存在する場合、その処理毎に、処理順位に基づいてステップS23以降で順次、処理されることとなる)。

【0054】ステップS24において、復号処理部43は、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理を完了することは不可能と判定した場合(タイム1-2の時間内に、処理が完了しないと判定した場合)、ステップS26において、復号処理部43は、他のコンテンツデータ単位の処理方法をメタデータに記述されている取扱情報から認識する。

【0055】取扱情報には、他のコンテンツデータ単位の処理方法が設定されており、データ送信装置21で設定されてメタデータに記述される。

【0056】取扱情報に記述されている他のコンテンツデータ単位の処理方法には、例えば次のような方法がある。処理方法1は、復号処理部43は、最優先処理が全て終了した後に、他のコンテンツデータ単位の処理を開始する処理方法(遅延処理)である。この場合、復号処理部43は、他のコンテンツデータ単位を遅延処理することをデータ処理判断部42に通知する。

【0057】処理方法2は、復号処理部43は、他のコンテンツデータ単位の処理を実行せずに、他のコンテンツデータ単位の処理を実行しないことをデータ処理判断部42に通知のみする処理方法である。

【0058】処理方法3は、復号処理部43は、他のコンテンツデータ単位の処理を実行しないだけでなく、他のコンテンツデータ単位の処理を実行しないことをデータ処理判断部42に通知もしない処理方法であり、復号処理部43は、他のコンテンツデータ単位が転送されてきたとしても、他のコンテンツデータ単位を無視して最優先処理を続行する。

【0059】ステップS26において、復号処理部43は、取扱情報に処理方法1が設定されていると認識した

場合、ステップS27に進み、復号処理部43は、他のコンテンツデータ単位を遅延処理することを決定する。また、復号処理部43は、他のコンテンツデータ単位を遅延処理することをデータ処理判断部42に通知する。その後、処理はステップS19に戻り、同様の処理が繰り返し実行される。最優先処理が全て終了した場合、復号処理部43は、図6のようにデータ処理判断部42から転送される遅延処理データ単位の復号関連処理を実行する。

【0060】ステップS26において、復号処理部43は、取扱情報に処理方法2が設定されていると認識した場合、ステップS28に進み、復号処理部43は、他のコンテンツデータ単位を処理せずに、データ処理判断部42に他のコンテンツデータを処理しないことを通知する。その後、処理はステップS19に戻り、同様の処理が繰り返し実行される。

【0061】ステップS26において、復号処理部43は、取扱情報に処理方法3が設定されていると認識した場合、ステップS29に進み、復号処理部43は、他のコンテンツデータ単位を処理しないだけでなく、データ処理判断部42になにも通知しない。その後、処理はステップS19に戻り、同様の処理が繰り返し実行される。

【0062】ステップS19において、復号処理部43が復号関連処理は全て終了したと判定した場合、処理は終了される。

【0063】なお、取扱情報は、データ送信装置21において設定され、メタデータに記述されるとしたが、データ処理判断部42に取扱情報を予め与えておき、データ処理判断部42は、他のコンテンツデータ単位を認識した場合、与えられた取扱情報に基づいて処理を行うことが可能である。

【0064】また、復号処理部43が最優先処理を実行している場合でも、さらに処理順位が上位にある処理が新しくデータ送信装置21から送信され、データ処理判断部42から復号処理部43に転送された場合、復号処理部43は、最優先処理を中止し、新しく転送されたコンテンツデータを処理するように取扱情報に設定することも可能である。

【0065】図7は、本発明を適用したコンテンツ配信システムの構成を示す図である。コンテンツプロバイダ51は、コンテンツサーバ52を管理しており、コンテンツデータおよびメタデータを作成する。コンテンツプロバイダ51が作成したコンテンツデータおよびメタデータは、サービスプロバイダ53が管理するサーバ54に供給される。コンテンツデータは、映画、音楽などのデジタルデータであり、メタデータにはそれらのデータに関する情報が記述される。

【0066】サービスプロバイダ53は、ネットワーク22を介して、契約者である利用者55に対してコンテ

ンツデータおよびメタデータを送信する。

【0067】利用者55は、サービスプロバイダ53から送信されたコンテンツデータおよびメタデータを、自らが操作する利用者端末56において利用する。

【0068】決済センタ57は、決済サーバ58を管理しており、利用者55に対してコンテンツデータの使用権情報を発行するとともに、使用権情報の代金の決済処理を行う。また、決済センタ57は、利用者55から支払われた代金を、コンテンツプロバイダ51と、サービスプロバイダ53の間で予め設定された契約に基づいて分配する。

【0069】図8は、コンテンツサーバ52の構成例を示すブロック図である。コンテンツサーバ52は、データキャプチャ装置71、データ編集装置72、メタデータ生成装置73、データ暗号化装置74、データ記憶装置75、およびデータ送信装置76より構成される。

【0070】データキャプチャ装置71は、外部から取り込んだデータを、コンテンツサーバ52の各装置が処理できるデータ形式に変換する。

【0071】データ編集装置72は、データキャプチャ装置71から転送されたデータから、利用者55に提供するコンテンツデータを作成する装置である。また、データ編集装置72は、メタデータ生成装置73が生成したメタデータをコンテンツデータに付加する。

【0072】データ暗号化装置74は、データ編集装置72から転送されたコンテンツデータおよびメタデータに暗号関連処理を施す。

【0073】データ記憶装置75は、データ暗号化装置74により暗号関連処理が施されたメタデータおよびコンテンツデータを記憶し、必要に応じてデータ送信装置76に転送する。

【0074】データ送信装置76は、サービスプロバイダ53が管理するサービスサーバ54にコンテンツデータおよびメタデータを送信する。なお、具体的な各装置の処理については、図16のフローチャートを参照して後述する。

【0075】図9は、データ暗号化装置74の詳細な構成例を示すブロック図である。データ暗号化装置74は、入出力インタフェースブロック91、データ処理判断ブロック92、データ記憶ブロック93、乱数生成ブロック94、および暗号化処理ブロック95から構成される。さらに、暗号化処理ブロック95は、暗号化処理サブブロック96、デジタル署名生成サブブロック97、およびハッシュ値計算サブブロック98より構成される。

【0076】入出力インタフェースブロック91は、データ編集装置72から供給されるメタデータおよびコンテンツデータを、データ処理判断ブロック92に転送する。

【0077】データ処理判断ブロック92は、データ暗

号化装置74の全体の動作を制御する。

【0078】データ記憶ブロック93は、暗号化処理ブロック95において、暗号関連処理が施されたメタデータおよびコンテンツデータや、処理に必要なデータを、適宜、記憶する。

【0079】乱数生成ブロック94は、データ処理判断ブロック92からの指令により乱数を生成し、暗号化処理ブロック95に供給する。乱数生成ブロック94が生成する乱数は、暗号化アルゴリズムであるDES (Data Encryption Standard)、RSA (Rivest-Shamir-Adleman scheme) などの共通鍵暗号方式で暗号関連処理する場合の鍵として利用される。

【0080】暗号化処理ブロック95は、コンテンツの暗号化およびデジタル署名の生成処理を行う。この暗号化処理ブロック95の暗号化処理サブブロック96は、DES、RSAなどの暗号化アルゴリズムによりコンテンツデータの暗号化処理を行う。

【0081】デジタル署名生成サブブロック97は、DSA (Digital Signature Algorithm) などによるデジタル署名の生成アルゴリズムによりデジタル署名を生成する。デジタル署名は、データの改竄のチェックおよびデータの制作者を認証するためのデータである。

【0082】ハッシュ値計算サブブロック98は、ハッシュ関数による計算を行う。ハッシュ関数は、送信するデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、出力であるハッシュ値から入力データを復元することが難しく、また、同一の出力結果のハッシュ値を持つ入力データを探し出すことが困難である（一方である）特徴を有する。

【0083】ここで、デジタル署名の生成および検証について説明する。デジタル署名の生成者は、送信するデータから特定のアルゴリズムを用いて、メッセージダイジェストを作成する（ハッシュ値計算サブブロック98により、送信するデータに、ハッシュ関数を適用し、メッセージダイジェストを作成する）。デジタル署名の生成者は、自分の秘密鍵（乱数生成ブロック94により生成された乱数）を使って、このメッセージダイジェストと送信するデータの全文を暗号化し、利用者に送信する。

【0084】一方、データの利用者は、データを受信し、デジタル署名の生成者が提供する公開鍵を利用して、暗号化されているデータの全文、およびメッセージダイジェストを復号する。次に、データの利用者は復号したデータの全文から、デジタル署名の生成者と同じ方式（同一のハッシュ関数）でメッセージダイジェストを作成する。生成されたメッセージダイジェストと受信されたメッセージダイジェストを比較することにより、デジタル署名の検証が行なわれる。すなわち、データの送信者から送信され、受信者が復号したメッセ

ジダイジェストと、受信者が復号したデータの全文から、送信者と同じ方式により作成したメッセージダイジェストが等しければ、そのデータは改竄などの不正な処理が行われていないことを表す。

【0085】なお、データ暗号化装置74において、説明の便宜上、暗号化処理サブブロック96、およびデジタル署名生成サブブロック97は暗号関連処理を行うことが可能であるとしたが、通常は、復号関連処理も行うことが可能である。すなわち、暗号化処理サブブロック96はデータの暗号化および復号が可能であるし、デジタル署名生成サブブロック97はデジタル署名の生成および検証が可能である。

【0086】さらに、後述する図14の暗号化処理ブロック163に配置されている暗号化処理部186を構成するサブブロックも、データ暗号化装置74を構成するサブブロックと同様に、復号関連処理だけでなく暗号関連処理を実行することができる。また、サービスサーバ54に配置されているデータ暗号化装置114も上述したコンテンツサーバ52に配置されているデータ暗号化装置74、および暗号化処理ブロック163と同様に、復号関連処理だけでなく暗号関連処理を実行することができる。これにより、それぞれの装置間で送受信されるデータに、改竄などの不正な処理が行われることを防ぐことが可能となる。

【0087】上述したような暗号関連処理が施されたコンテンツデータおよびメタデータは、サービスプロバイダ53が管理するサービスサーバ54に送信される。

【0088】図10は、サービスサーバ54の構成例を示すブロック図である。サービスサーバ54は、データ送受信装置111、データ編集装置112、メタデータ生成装置113、データ暗号化装置114、コンテンツプロモーションサーバ115、およびデータ記憶装置116より構成される。

【0089】データ送受信装置111は、コンテンツサーバ52から送信されるコンテンツデータおよびメタデータを受信する。また、データ送受信装置111は、利用者端末56に対し、ネットワーク22を介してコンテンツデータおよびメタデータを送信する。データ送受信装置111は、コンテンツデータおよびメタデータを送信するタイミングを判断する。送信するタイミングは、例えば、利用者55からの要求に応じて送信する場合や、メタデータに記述されているタイミングで送信する場合などがある。

【0090】データ編集装置112は、サービスサーバ54の各装置で処理されたデータを編集し、利用者55に提供する形態にデータを編集する。

【0091】メタデータ生成装置113は、メタデータを生成する。メタデータ生成装置113が生成するメタデータには、サービスプロバイダ53がコンテンツデータを利用者55に提供する際に、サービスプロバイダ5

3が利用者55に対して通知する情報が記述される。

【0092】データ暗号化装置114は、メタデータ生成装置113が生成したメタデータにデジタル署名を生成するなどの暗号関連処理を行う。データ暗号化装置114の詳細な構成は、図8に示すコンテンツサーバ52のデータ暗号化装置74（図9）の構成と同様である。

【0093】コンテンツプロモーションサーバ115は、サービスプロバイダ53が利用者55に提供するコンテンツの一覧情報を作成するとともに、ディスクカウント情報などを利用者55の要求に応じて提供する。コンテンツプロモーションサーバ115は、WWWサーバとして設置され、利用者55は利用者端末56に装備されているブラウザを利用することにより、コンテンツプロモーションサーバ115が提供するサービスを受けることができる。さらに、コンテンツプロモーションサーバ115は、利用者55からの電話による問い合わせに対応できるようにもなっている。

【0094】データ記憶装置116は、データ編集装置112で編集されたデータを記憶し、利用者55からの要求に応じて、データ送受信装置111に対してコンテンツデータおよびメタデータを転送する。なお、具体的な各装置の処理については、図19のフローチャートを参照して後述する。

【0095】図11は、決済センタ57が管理している決済サーバ58の構成例を示すブロック図である。決済サーバ58は、データ送受信装置131、ライセンス装置132、ユーザ管理装置133、著作権管理装置134、課金装置135、および決済装置136より構成される。

【0096】データ送受信装置131は、利用者端末56から、ネットワーク22を介して通知されるコンテンツデータの著作権の購入要求情報を受信するとともに、コンテンツプロバイダ51およびサービスプロバイダ53に対して、利用者55から回収した代金の課金情報を送信する。

【0097】ライセンス装置132は、利用者55からコンテンツデータの著作権購入が要求された場合、著作権情報の発行処理を行う。

【0098】ユーザ管理装置133は、サービスプロバイダ53から、コンテンツデータの提供を受ける契約をしている利用者55、およびその利用者55が操作する利用者端末56の情報を管理する。利用者55および利用者端末56の情報には、利用者端末56に含まれるセリットトップボックスの契約日、契約条件、サービスの利用情報などが含まれる。

【0099】著作権管理装置134は、コンテンツデータの著作権の他、サービスプロバイダ53から提供される利用者55が利用可能なコンテンツデータの利用形態、および利用者55によるコンテンツデータの購入履歴

歴などを管理する。

【0100】課金装置135は、コンテンツデータの著作権情報の料金情報を管理するとともに、利用者55に対して、課金情報を通知する。

【0101】決済装置136は、課金装置135から決済処理の要求をうけて、決済処理を行う。具体的な決済方法には、クレジットカードによる決済方法、プリペイド型の電子マネーによる決済方法が含まれる。なお、決済サーバ58の著作権情報の発行処理については、図21および22のフローチャートを参照して後述する。

【0102】図12は、利用者55が管理する利用者端末56の構成例を示すブロック図である。利用者端末56は、セットトップボックス151（以下、適宜、STB151と称する）、およびデータ再生装置152より構成される。

【0103】STB151は、ネットワーク22を介して、サービスサーバ54、および決済サーバ58との間でデータの送受信を行う。STB151の詳細な構成例は図13に示す。

【0104】データ再生装置152は、サービスサーバ54から提供され、STB151が処理したコンテンツデータを再生する装置である。データ再生装置152は、例えば、テレビジョン受像機、パーソナルコンピュータなどの電子機器により構成される。

【0105】図13は、セットトップボックス151の構成例を示すブロック図である。STB151は、データ送受信ブロック161、コントローラ162、暗号化処理ブロック163、フラッシュメモリ164、および外部RAM（Random Access Memory）165から構成される。

【0106】データ送受信ブロック161は、サービスサーバ54から、ネットワーク22を介して送信されるコンテンツデータおよびメタデータ、若しくは決済サーバ58から送信されるコンテンツデータの著作権情報などを受信する。また、データ送受信ブロック161は、サービスサーバ54に対するデータの送信要求、および決済サーバ58に対する著作権情報を要求する情報などを送信するとともに、データ再生装置152に、処理結果を転送する。

【0107】コントローラ162は、ソフトウェアにより制御され、STB151全体の動作を制御する。

【0108】暗号化処理ブロック163は、データ送受信ブロック161が受信するコンテンツデータおよびメタデータの復号関連処理を行う。詳細な構成例については図14に示す。

【0109】フラッシュメモリ164は、STB151の電源遮断後もデータを記憶している不揮発性のメモリである。フラッシュメモリ164には、各ブロックが処理するために必要なデータ、および各ブロックの処理結果が、適宜、記憶される。

【0110】外部RAM165は、暗号化処理ブロック163による処理結果、システム制御データ、および課金処理結果等を記憶する。

【0111】図14は、暗号化処理ブロック163の詳細な構成例を示すブロック図である。暗号化処理ブロック163は、入出力インタフェースブロック181、マイクロプロセッサ182、RAM183、乱数生成ブロック184、フラッシュメモリ185、および暗号化処理部186より構成される。さらに、暗号化処理部186は、暗号化処理サブブロック187、デジタル署名検証サブブロック188、およびハッシュ値計算サブブロック189より構成される。

【0112】入出力インタフェースブロック181は、データ送受信ブロック161が受信したコンテンツデータおよびメタデータのうち、コントローラ162により復号関連処理が必要であると判断され、暗号化処理ブロック163に転送されるデータを受信する。入出力インタフェースブロック181は、コントローラ161から供給されるデータを、マイクロプロセッサ182に転送する。マイクロプロセッサ182は、暗号化処理ブロック163の全体の動作を制御する。

【0113】RAM183は、マイクロプロセッサ182が処理をするのに必要なプログラムを記憶している。また、RAM183には、マイクロプロセッサ182が処理した結果が記憶される。

【0114】乱数生成ブロック184は、マイクロプロセッサ182からの指令により乱数を生成し、暗号化処理部186に供給する。乱数生成ブロック184が生成した乱数は、DES、RSAなどの共通鍵暗号方式で暗号関連処理が施されたデータを、復号する場合の鍵として利用される。

【0115】フラッシュメモリ185は、不揮発性のメモリであり、内部に図示せぬコントローラを保持している。マイクロプロセッサ182において動作するソフトウェアの実行コード、復号関連処理に必要な各種データ、購入したコンテンツデータの著作権情報などが記憶される。

【0116】暗号化処理部186は、コンテンツデータおよびメタデータの復号関連処理を行う。暗号化処理部186は、さらに、以下の機能を提供するサブブロックにより構成される。

【0117】暗号化処理サブブロック187は、DES、RSAなどの暗号化アルゴリズムにより暗号化されたコンテンツデータの復号処理を行う。

【0118】デジタル署名検証サブブロック188は、DSAなどによるデジタル署名アルゴリズムによりデジタル署名が付加されたコンテンツデータおよびメタデータのデジタル署名検証処理を行う。

【0119】ハッシュ値計算サブブロック189は、ハッシュ関数による計算を行う。

【0120】図15は、暗号化処理ブロック163が、コントローラ162等と送受信するデータ形式の例を示す図である。コントローラ162は、暗号化処理ブロック163に対して、図15のデータ形式のコマンドデータで処理を要求する。また、暗号化処理ブロック163は、コマンドデータに基づいて各ブロックを制御し、所定の処理を実行させるとともに、コマンドデータにより処理を要求したコントローラ162に対して、図15のデータ形式のレスポンスデータで処理結果を送信する。

【0121】フィールド1は、データ種識別フィールドであり、コマンドデータ、またはレスポンスデータの種類の記述される。

【0122】フィールド2は、データ番号フィールドであり、コマンドデータ、またはレスポンスデータの番号が記述される。

【0123】フィールド3は、データ長フィールドであり、データフィールド4に記述されるデータの長さが記述される。

【0124】フィールド4は、データフィールドであり、コマンドデータとして処理を要求するデータ、またはレスポンスデータとして送信する処理結果のデータが記述される。以下、コマンドデータ、およびレスポンスデータの例を説明する。

【0125】データ番号フィールドに記述される番号が1であるコマンド1は、デジタル署名の検証処理の要求を表している。フィールド4のデータフィールドに記述されているデータに対して、暗号化処理ブロック163は、データが改竄されていないかを検証し、その処理結果をレスポンス1として、データ処理を要求したブロックに送信する。

【0126】コマンド2は、デジタル署名の生成処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されているデータに対して、デジタル署名を付加したデータをレスポンス2として、データ処理を要求したブロックに送信する。

【0127】コマンド3は、暗号化されているデータの復号処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されている暗号化されているデータに対して、復号処理を行い、復号したデータをレスポンス3として、データ処理を要求したブロックに送信する。

【0128】コマンド4は、暗号化処理の要求を表している。暗号化処理ブロック163は、フィールド4のデータフィールドに記述されているデータを暗号化し、暗号化したデータをレスポンス4として、データ処理を要求したブロックに送信する。

【0129】コマンド5は、ハッシュ値計算の要求を表している。ハッシュ値計算サブブロック189は、フィールド4のデータフィールドに記述されているデータ、

およびアルゴリズムをもとに、ハッシュ関数による計算を行い、計算結果のデータをレスポンス5として、データ処理を要求したブロックに送信する。

【0130】コマンド6は、処理の停止要求を表している。このコマンドを受信した場合、暗号化処理ブロック163は、その時点で行っている処理を停止し、停止した旨の通知をレスポンス6として処理の停止を要求するブロックに送信する。

【0131】コマンド7は、使用権情報の送信要求を表している。このコマンドを受信した場合、暗号化処理ブロック163は、自らがフラッシュメモリ185に保持している使用権情報を暗号化して、決済サーバ58にレスポンス7として送信する。

【0132】コマンド20は、外部装置または他のブロックから送信されるメッセージである。そのデータフィールドには、コントローラ162などからメッセージが入力される。

【0133】レスポンス30は、暗号化処理ブロック163が、外部装置または他のブロックに対して送信するメッセージである。

【0134】以下、コンテンツプロバイダ51が提供するコンテンツデータを、利用者55が利用するまでの一連の処理についてフローチャートを参照して説明する。

【0135】始めに、図16のフローチャートを参照して、コンテンツプロバイダ51が管理するコンテンツサーバ52の処理を説明する。

【0136】ステップS41において、データキャプチャ装置71は、ビデオカメラ、およびオーディオレコーダなどから取り込んだアナログデータ、またはデジタルデータを、コンテンツサーバ52の各装置が処理できるデータ形式に、デジタル化処理、または圧縮などの処理を行う。

【0137】ステップS42において、データ編集装置72は、データキャプチャ装置71から取得したデータから、コンテンツプロバイダ51の指令に基づいて、利用者55に提供するコンテンツデータを作成する。また、データ編集装置72は、メタデータ生成装置73が生成するメタデータをコンテンツデータに付加する。

【0138】図17は、メタデータ生成装置73が生成するメタデータの例を示す図である。図17(A)のメタデータ1の例において、フィールド1には、コンテンツプロバイダ51を特定するコンテンツプロバイダIDが2、メタデータ1に対応するコンテンツデータ(以下、適宜、コンテンツデータ1と称する。後述する他のメタデータが付加されるコンテンツデータの場合も同様とする)を特定するコンテンツIDが1、コンテンツデータ1の著作権の権利発生日時が西暦2000年1月1日と記述されている。

【0139】フィールド2には、利用者55によるコンテンツデータ1の利用形態が記述される。ここでは、利

用形態1としてストリーミング、利用形態2として買い取り、および利用形態3として期間限定1年の利用形態が記述されている。ストリーミングによる利用形態は、利用者端末56において、サービスサーバ54からコンテンツデータ1を受信しながらリアルタイムで再生する利用形態であり、利用回数が1回のみの利用形態である。買い取りによる利用形態とは、期間および利用回数が無制限である利用形態であり、利用者端末56に送信されたコンテンツデータ1は、利用者端末56の図示せぬ記録媒体に記録される。また、期間限定1年の利用形態とは、コンテンツデータ1が利用者端末56の図示せぬ記録媒体に記録された後、利用者55は期間が1年以内であれば、回数は無制限にコンテンツデータ1を利用することが可能な形態である。

【0140】フィールド3には、コンテンツデータ1の利用形態毎の料金が記述される。ここでは、コンテンツデータ1を利用形態1のストリーミングにより利用した場合、料金は20円とされ、コンテンツデータ1を利用形態2の買い取りにより利用した場合、料金は100円とされ、コンテンツデータ1を利用形態3の期間限定1年の利用形態により利用した場合、料金は50円とされている。利用者55は、フィールド3に記述される料金に基づいて、決済センタ57に対して使用権情報の代金を支払う。

【0141】フィールド4には、コンテンツデータ1の形式的な情報が記述される。ここでは、コンテンツデータ1の総データ量は150MBで、利用者端末56のデータ再生装置152で再生した場合の再生時間は10分と記述されている。また、コンテンツデータ1は、MPEG (Moving Picture Experts Group) 2の規格で圧縮されているビデオデータであり、データ転送速度は2Mbpsと記述されている。

【0142】フィールド5には、データ暗号化装置74がコンテンツデータおよびメタデータに施した暗号関連処理の情報が記述される。この例で、デジタル署名の生成アルゴリズムはDSA、コンテンツデータ1の暗号化アルゴリズムはDES、コンテンツデータ1の暗号化のデータ単位は256KBと記述されている。暗号化のデータ単位は、1つの暗号化の鍵で連続して暗号化する場合のデータの大きさである。暗号化に利用した鍵はさらに別の鍵(メタ鍵)で暗号化されており、メタ鍵は決済センタ57に委託され、利用者55が使用権情報を購入した場合、決済サーバ58から使用権情報とともに、後述する図23の使用権情報のデータ形式で、利用者55に提供される。

【0143】フィールド6には、利用者端末56のSTB151に含まれる暗号化処理ブロック163が処理するコンテンツデータ1に関する情報が記述される。この例で、暗号化処理ブロック163に要求される復号関連処理は、コンテンツデータ1の各暗号化単位ブロック毎に

付加されているデジタル署名の検証処理、および暗号化されているコンテンツデータ1の復号処理である。

【0144】まず、STB151のコントローラ162が、暗号化処理ブロック163に対して転送するデータの転送周期が記述されている。暗号化処理ブロック163が処理するデジタル署名の検証が必要なデータの転送周期は1秒とされ、また、復号処理が必要な暗号化されているコンテンツデータ1の転送周期も1秒とされている。

【0145】次に、暗号化処理ブロック163が処理する各処理の優先度を示す処理順位が設定されている。ここでは、デジタル署名の検証の処理順位は2、コンテンツデータ1の復号処理の処理順位は1と設定されている。2つの処理が暗号化処理ブロック163に要求された場合、ここで設定されている処理順位により、暗号化処理ブロック163はコンテンツデータ1の復号処理を優先して処理することになる。

【0146】さらに、フィールド6には、各処理の取扱情報が記述される。取扱情報は、第1の処理より優先度が高い第2の処理があり、第1の処理を実行することができない場合の第1の処理の取り扱い方法についての情報である。この例の場合、デジタル署名の検証処理より、処理順位が高い(リアルタイム性が高い)第2の処理が存在し、STB151の暗号化処理ブロック163は、第2の処理が終了し、次の第2の処理が必要なデータが転送されてくるまでの間に、デジタル署名の検証を行うことができない場合、デジタル署名の検証処理は、第2の処理が全て終了した後に処理する(遅延処理する)と設定されている。また、暗号化処理ブロック163は、遅延処理することをコントローラ162に通知するようにも設定されている。

【0147】また、暗号化されているコンテンツデータ1の復号処理より、処理順位が高い(リアルタイム性が高い)第2の処理が存在し、STB151の暗号化処理ブロック163は、第2の処理が終了し、次の第2の処理が必要なデータが転送されてくるまでの間に、コンテンツデータ1の復号処理を行うことができない場合も、デジタル署名の検証処理と同様に、遅延処理を行い、またコントローラ162に通知するように設定されている。

【0148】図17(B)のメタデータ2の例において、フィールド1およびフィールド5に記述されている内容はメタデータ1と同一の内容である。フィールド6に記述されている取扱情報には、デジタル署名の検証処理より、処理順位が高い(リアルタイム性が高い)第2の処理が存在し、STB151の暗号化処理ブロック163は、第2の処理が終了し、次のデジタル署名の検証が必要なデータが転送されてくるまでの間に、デジタル署名の検証を行うことができない場合、デジタル署名の検証処理は、無視すると設定され、記述されてい

る。

【0149】図16に戻って、ステップS43において、データ暗号化装置74は、データ編集装置72から転送されるコンテンツデータおよびメタデータに暗号関連処理を施す。

【0150】すなわち、乱数生成ブロック94は、暗号化鍵（コンテンツデータ用）として所定のビット数の乱数を生成し、暗号化処理サブブロック96に供給する。

【0151】暗号化処理サブブロック96は、乱数生成ブロック94が生成した乱数を暗号鍵としてコンテンツデータを暗号化するとともに、使用権情報に配置されて決済サーバ58から利用者端末56に対して送信されるメタ鍵を使用して、暗号化鍵（コンテンツデータ用）をDESなどの共通鍵暗号方式で暗号化する。

【0152】ハッシュ値計算サブブロック98は、コンテンツサーバ52がサービスプロバイダ53に対して送信するメタデータにハッシュ関数を適用してハッシュ値を算出する。

【0153】デジタル署名生成サブブロック97は、ハッシュ値計算サブブロック98が抽出したハッシュ値を、乱数生成ブロック94が生成した乱数よりなる暗号化鍵を利用して暗号化し、デジタル署名を生成する。

【0154】ステップS44において、データ記憶装置75は、データ暗号化装置74により暗号関連処理が施されたデータを記憶し、必要に応じてデータ送信装置76に出力する。

【0155】ステップS45において、データ送信装置76は、サービスプロバイダ53が管理するサービスサーバ54にメタデータおよびコンテンツデータを送信する。

【0156】図18は、ステップS45の処理により送信されるデータのフォーマットの例を示す。レイヤ1は、ステップS42の処理により生成されたメタデータ、ステップS43の処理により付加されたメタデータ用のデジタル署名、ステップS43の処理で用いられた暗号化鍵（コンテンツデータ用）、並びにコンテンツデータにより構成される。コンテンツデータは、さらに、レイヤ2としての暗号化単位ブロックにより構成されている。暗号化単位ブロックは、コンテンツデータ1、およびコンテンツデータ2の場合、256KB毎のブロックとされている。レイヤ2の暗号化単位ブロックはさらに、レイヤ3としての、256KBのデータ長のブロックと、デジタル署名とで構成されている。従って、この例では、この暗号化データに付加されているデジタル署名を検証することにより、コンテンツデータの各暗号化単位ブロックに、改竄などの不正処理が行われているか否かを判断することができる。

【0157】次に、図19のフローチャートを参照して、サービスプロバイダ53が管理するサービスサーバ54の処理を説明する。

【0158】ステップS61において、データ送受信装置111は、コンテンツサーバ52から、暗号関連処理が施されたコンテンツデータおよびメタデータを受信する。

【0159】ステップS62において、メタデータ生成装置113は、送信されてきたメタデータを確認し、元のデータを変更し、新たなメタデータを生成する。すなわち、このときデータ暗号化装置114は、コンテンツプロバイダ51から決済サーバ58を介して予め取得したメタ鍵を利用して、送信されてきた暗号化鍵（コンテンツデータ用）（図18）を復号し、復号した暗号化鍵（コンテンツデータ用）（図18）を利用してデジタル署名（メタデータ用）（図18）を復号する。そして、メタデータ生成装置113は、復号して得られたメタデータと、平文で送信されてきたメタデータを比較し、両者が一致していること、すなわち、メタデータが改竄されていないことを確認する。

【0160】さらに、メタデータ生成装置113は新たにメタデータを生成する。このメタデータは、コンテンツサーバ52が生成したメタデータ1（図17（A））およびメタデータ2（図17（B））のフィールド1およびフィールド3の内容を、サービスプロバイダ53が利用者55に通知する情報に書き換えたデータである。メタデータ3およびメタデータ4の内容は、サービスプロバイダ53が決定する。

【0161】図20は、図17に示されるコンテンツプロバイダ51が生成したメタデータを、ステップS62の処理で、メタデータ生成装置113が変更して生成したメタデータの例を示す。図17（A）のメタデータ1を変更して生成されたメタデータ3（図20（A））の例においては、フィールド1には、サービスプロバイダ53を特定するサービスプロバイダIDが1、メタデータ3を作成した日時が西暦2000年1月2日と記述されている。

【0162】フィールド3に記述されている料金には、図17（A）に示すメタデータ1のフィールド3に記述されている料金に、サービスプロバイダ53が利用者55に対してコンテンツデータを送信する送信料が付加されている。メタデータ3では、料金は、コンテンツデータをストリーミングの利用形態により利用する場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、サービスプロバイダ53が受け取る送信料の10円が付加されて30円とされ、コンテンツデータを買取りの利用形態により利用する場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、サービスプロバイダ53が受け取る送信料の50円が付加されて150円とされ、コンテンツデータを期間限定1年の利用形態により利用する場合は、コンテンツプロバイダ51が受け取るコンテンツデータの料金に、サービスプロバイダ53が受け取る送信料の30円が付加さ

れて80円とされている。

【0163】図17(B)のメタデータ2を変更して生成された図20(B)のメタデータ4の例においても、メタデータ3の場合と同様の変更がメタデータ生成装置113によりされている。

【0164】ステップS63において、データ暗号化装置114は、新たに生成したメタデータのハッシュ値を演算し、それを暗号化鍵(コンテンツデータ用)で暗号化し、新たなデジタル署名を生成し、ステップS62の処理で生成された新たなメタデータに付加する。データ暗号化装置114の暗号関連処理は、コンテンツサーバ52のデータ暗号化装置74の処理と同様に行われる。

【0165】ステップS64において、データ編集装置112は、サービスサーバ54の各装置で処理されたデータを編集し、利用者55に提供するコンテンツデータを作成する。このため、暗号化装置114は、送信されてきたコンテンツデータを暗号化鍵(コンテンツデータ用)で一旦復号する。その後データ編集装置112により行われる編集には、コンテンツサーバ52から送信されたコンテンツデータにステップS62の処理で生成されたメタデータを付加する処理、または複数のコンテンツデータを統合し、1つのコンテンツデータにまとめて利用者55に提供するアルバム化などの処理がある。編集後のコンテンツデータは、データ暗号化装置114により暗号化鍵(コンテンツデータ用)を用いて再び暗号化される。

【0166】ステップS65において、データ記憶装置116は、データ編集装置112で編集され、データ暗号化装置114により暗号化されたデータを記憶する。

【0167】ステップS66において、データ送受信装置111は、利用者55が管理する利用者端末56から、メタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。その後、データ送受信装置111が、メタデータの送信が要求されたと判定した場合、処理はステップS67に進む。

【0168】ステップS67において、データ送受信装置111は、利用者55が要求するコンテンツデータに対応するメタデータを、データ記憶装置116から取得し、ネットワーク22を介して利用者端末56に送信する。データ送受信装置111が送信するメタデータを受信した利用者端末56のSTB151は、メタデータに記述されている内容を確認し、コンテンツデータの復号関連処理の準備をする。STB151の詳細な処理については後述するが、その後、STB151からコンテンツデータの送信が要求されてくる。

【0169】そこで、ステップS68において、データ送受信装置111は、利用者端末56からコンテンツデータの送信が要求されたか否かを判定する。

【0170】データ送受信装置111が、利用者端末56からコンテンツデータの送信が要求されたと判定した場合、処理はステップS69に進み、データ送受信装置111は、データ記憶装置116に記憶されているコンテンツデータを、ネットワーク22を介して利用者端末56に送信する。

【0171】次に、決済センタ57が管理する決済サーバ58が、利用者端末56に対して行うコンテンツデータの使用権情報の発行処理について、図21および図22のフローチャートを参照して説明する。

【0172】ステップS81において、ライセンス装置132は、利用者端末56からコンテンツデータの使用権情報の購入が要求されたか否かを判定し、要求されたと判定するまで待機する。ライセンス装置132が、利用者端末56から使用権情報の購入が要求されたと判定した場合、処理はステップS82に進む。

【0173】ステップS82において、ライセンス装置132は、使用権情報の購入を要求している利用者55は、サービスプロバイダ53からコンテンツデータの提供を受ける契約をしているか否かを確認するため、利用者端末56のSTB151から送信される情報に基づいて、STB151は契約対象の機器であるか否かをユーザ管理装置133に問い合わせる。この問い合わせに応じて、ユーザ管理装置133は、自分自身が管理している契約情報から、使用権情報の購入を要求するSTB151は、契約対象の機器であるか否かを検索する。すなわち、このシステムでは、利用者55はコンテンツデータの提供を受ける前に、サービスプロバイダ53と予め契約をする必要がある。契約情報は、サービスプロバイダ53から決済センタ57に供給され、ユーザ管理装置133に登録される。

【0174】ステップS83において、ライセンス装置132は、ステップS82のユーザ管理装置133の検索結果を判定する。ライセンス装置132は、使用権情報の購入を要求しているSTB151は、契約対象の機器でないと判定した場合、利用者端末56に対して使用権情報を販売することができないことを通知し、処理を終了する。

【0175】ライセンス装置132が、使用権情報の購入を要求しているSTB151は、契約対象の機器であると判定した場合、処理はステップS84に進み、ライセンス装置132は、データ送受信装置131からネットワーク22を介してSTB151の暗号化処理ブロック163と相互認証を行い、セッション鍵を共有する。

【0176】ステップS85において、ライセンス装置132は、相互認証が成立したか否かを判定し、相互認証が成立していないと判定した場合、処理を終了する。

【0177】ステップS85において、ライセンス装置132が、相互認証が成立したと判定した場合、処理はステップS86に進み、ライセンス装置132は、STB1

51から送信される要求内容に基づいて、使用権情報の発行が可能であるか否かを著作権管理装置134に問い合わせる。STB151から送信される要求内容には、利用者55が利用を希望するコンテンツデータのコンテンツID、コンテンツデータの利用形態、および使用権情報の代金の決済方法が含まれる。(決済方法がクレジットカードによる決済の場合、クレジットカードのカード番号が、また、決済方法がプリペイドカード型の電子マネーによる決済の場合、プリペイドカードのカード番号が、それぞれ含まれる) このSTB151から送信される要求情報は、改竄などの不正処理を防ぐため、暗号化処理ブロック163により暗号化されてSTB151から送信される。

【0178】ステップS87において、ライセンス装置132は、ステップS86で著作権管理装置134に問い合わせた結果を判定する。ライセンス装置132は、使用権情報の発行ができないと判定した場合、利用者端末56に使用権情報の発行ができないことを通知し、処理を終了する。

【0179】ステップS87において、ライセンス装置132が、使用権情報の発行が可能であると判定した場合、処理はステップS88に進み、ライセンス装置132は、課金装置135に対して課金処理を要求する。

【0180】ステップS89において、課金装置135は、自らが管理している料金情報から、利用者55が要求する使用権情報の代金を取得し、決済装置136に対して決済処理の要求をするとともに、利用者端末56に対して課金情報を通知する。

【0181】ステップS90において、課金装置135から決済処理の要求を受けた決済装置136は決済処理を行う。決済方法がクレジットカードによる決済の場合、決済装置136は、図示せぬクレジットカード会社の決済サーバに、使用権情報の購入を要求している利用者55のユーザID、および課金装置135が取得した使用権情報の代金を通知し、クレジット会社の決済サーバから、決済が可能であるか否かのメッセージを受け取る。決済装置136は、メッセージの結果を課金装置135に通知する。

【0182】利用者55が要求する決済方法が、プリペイドカード型の電子マネーによる決済の場合、決済装置136は、利用者55から通知されたカードIDと、自身自身が管理するプリペイドカードのカードIDを照合し、決済が可能であるか否かを判定する。決済装置136は、この判定結果を課金装置135に通知するとともに、決済が可能である場合、利用者55が使用しているプリペイドカード型の電子マネーの残高情報を更新する。

【0183】ステップS91において、課金装置135は、決済装置136から通知される情報により、決済が成立したか否かを判定する。決済が成立していないと判

定した場合、課金装置135は、決済が成立していないことを利用者端末56に通知し、処理を終了する。

【0184】ステップS91において、課金装置135は、決済が成立したと判定した場合、ライセンス装置132に決済が成立したことを通知する。

【0185】このときステップS92において、ライセンス装置132は、使用権情報をセッション鍵で暗号化し、ネットワーク22を介して利用者端末56に送信する。送信された使用権情報は、STB151の暗号化処理ブロック163によりセッション鍵で復号される。

【0186】図23は、使用権情報の例を示している。この使用権情報の例では、フィールド1には、利用者55に対してコンテンツデータの使用権情報の発行を許可するコンテンツプロバイダ51のIDが2、利用が許可されたコンテンツデータのコンテンツIDが1、および使用権の権利発生日時が西暦2000年1月2日と記述されている。

【0187】フィールド2にはコンテンツプロバイダ51により許可された利用形態がストリーミングであることが記述されており、フィールド3には、そのストリーミングによる利用形態の料金が30円とされている。

【0188】フィールド4には、メタ鍵が配置されている。通常、利用が許可されたコンテンツデータを復号するための鍵(暗号化鍵(コンテンツデータ用)(図18))は暗号化されており、メタ鍵はその暗号化鍵(コンテンツデータ用)(図18)を復号して取得するための鍵である。

【0189】フィールド5には、使用権情報全体のデジタル署名が付加される。

【0190】使用権情報は、STB151の暗号化処理ブロック163により、そのデジタル署名の検証が行われた後、暗号化処理ブロック163の内部に配置されているフラッシュメモリ185に記憶される。記憶された使用権情報は、コンテンツデータの復号関連処理において、適宜、利用される。

【0191】次に、使用権情報を取得した後のSTB151の処理について、図24乃至図26のフローチャートを参照して説明する。ここでは、STB151がメタデータ3およびコンテンツデータ3を受信して処理する場合について説明する。

【0192】ステップS111において、STB151のコントローラ162は、利用者55からの指令に基づいてサービスサーバ54に対して、使用権情報を購入したコンテンツデータ3に対応するメタデータ3の送信を要求する。

【0193】ステップS112において、データ送受信ブロック161は、サービスサーバ54から送信されたメタデータ3を、ネットワーク22を介して受信する。

【0194】ステップS112において、データ送受信ブロック161が受信したメタデータ3は、コントロー

ラ162に転送される。コントローラ162は、メタデータ3にはデジタル署名が付加されているため、デジタル署名の検証が必要であると認識し、メタデータ3を暗号化処理ブロック163に転送する。

【0195】ステップS113において、暗号化処理ブロック163のマイクロプロセッサ182は、転送されたメタデータ3のデジタル署名を検証し、メタデータ3の正当性を判断する。

【0196】すなわち、ハッシュ値計算サブブロック189は、平文で送られてきたメタデータ3にハッシュ関数を適用してハッシュ値を演算する。暗号化処理サブブロック187は、フラッシュメモリ185に記憶されているメタ鍵で暗号化鍵（コンテンツデータ用）を復号し、さらに、暗号化鍵（コンテンツデータ用）でデジタル署名を復号し、そこに含まれるハッシュ値を得る。デジタル署名検証サブブロック188は、ハッシュ値計算サブブロック189が、転送されたメタデータ3の全文からハッシュ関数を利用して算出したハッシュ値と、暗号化処理サブブロック187により復号されたハッシュ値を比較することにより、デジタル署名を検証する。なお、ハッシュ値計算サブブロック189が利用するハッシュ関数は、コンテンツサーバ52のハッシュ値計算サブブロック98や、サービスサーバ54のデータ暗号化装置114が利用するハッシュ関数と同一の関数である。

【0197】マイクロプロセッサ182は、デジタル署名検証サブブロック188が検証した結果を取得し、不正処理の有無を判定する。

【0198】ステップS114において、マイクロプロセッサ182は、メタデータ3が正常なデータ（改竄されていないデータ）であるかを判定し、不正処理を認識した場合（ハッシュ値が一致しない場合）、コントローラ162に通知する。コントローラ162は、不正処理の存在を利用者55に通知し、処理を終了する。

【0199】ステップS114において、マイクロプロセッサ182により、メタデータ3が正常なデータであることが確認された場合、処理はステップS115に進み、マイクロプロセッサ182は、受信したメタデータ3の内容を、決済センタ57から購入し、フラッシュメモリ185に記憶されている使用権情報の内容と比較する。これにより、データ送受信ブロック161が受信したメタデータ3は、利用者55が使用権情報を購入し、サービスサーバ54に送信を要求するコンテンツデータ3に対応するメタデータであるかがマイクロプロセッサ182により判定される。

【0200】ステップS116において、ステップS115でマイクロプロセッサ182が比較した結果がマイクロプロセッサ182により判定される。マイクロプロセッサ182は、メタデータ3の内容が使用権情報の内容と一致せず、正当性が確認できないと判定した場合、コ

ントローラ162に通知する。コントローラ162は、利用者55に対してメタデータ3に不正処理が存在していることを通知し、処理を終了する。

【0201】ステップS116において、マイクロプロセッサ182が、メタデータ3の内容と使用権情報の内容を比較し、メタデータ3の正当性を確認した場合、処理はステップS117に進み、マイクロプロセッサ182は、メタデータ3に含まれる暗号関連情報を確認し、コンテンツデータ3の復号関連処理の準備をする。

【0202】なお、この例の暗号化処理ブロック163は、DESのアルゴリズムで暗号化されているコンテンツデータ3を復号し、復号した結果を転送する速度は4Mbpsであり、またDSAのアルゴリズムで作成されているデジタル署名を検証する処理能力は1Mbpsであるとする。

【0203】ステップS117において、マイクロプロセッサ182は、メタデータ3のフィールド6に記述されている内容から、復号関連処理をリストアップする。この例の場合、マイクロプロセッサ182は、DSAのアルゴリズムで生成されて、コンテンツデータ3に付加されているデジタル署名の検証処理と、DESのアルゴリズムで暗号化されたコンテンツデータ3の復号処理をリストアップする。

【0204】ステップS118において、マイクロプロセッサ182は、メタデータ3のフィールド6に記述されている内容から、ステップS117の処理でマイクロプロセッサ182がリストアップしたデジタル署名の検証処理、およびコンテンツデータ3の復号処理は、いずれも処理が要求されるタイミングに周期性があると認識する。また、マイクロプロセッサ182は、それぞれの処理の処理順位を確認する。マイクロプロセッサ182は、デジタル署名の検証処理の処理順位は2と、コンテンツデータ3の復号処理の処理順位は1と設定されていることを認識し、コンテンツデータ3の復号処理を最優先処理に選択する。

【0205】ステップS119において、マイクロプロセッサ182は、メタデータ3のフィールド6の記述から、コントローラ162がコンテンツデータ3の復号処理をマイクロプロセッサ182に対して要求する周期（復号処理が必要なコンテンツデータ3のデータ単位が転送されてくる周期）は1秒であると認識し、その周期を基準周期に設定する（図6のタイム1およびタイム2は1秒となる）。

【0206】ステップS120において、マイクロプロセッサ182から、最優先処理を選択し、基準周期を設定した旨の通知を受けたコントローラ162は、サービスサーバ54に対してコンテンツデータ3の送信を要求する。

【0207】ステップS121において、データ送受信ブロック161は、ネットワーク22を介してコンテン

ッデータ3を受信する。

【0208】ステップS122において、データ送受信ブロック161からコンテンツデータ3の転送を受けたコントローラ162は、コンテンツデータ3のうちの復号処理が必要なデータ単位を、基準周期に基づいて暗号化処理ブロック163に転送する（図6の最優先処理データ単位1が転送される）。

【0209】ステップS123において、暗号化処理ブロック163は、最優先処理を開始し、コンテンツデータ3のデータ単位を復号する。暗号化処理ブロック163が復号したコンテンツデータ3は、適宜、データ再生装置152に転送される。

【0210】暗号化処理ブロック163に含まれる暗号化処理サブブロック187は、フラッシュメモリ185に記憶されている使用権情報からメタ鍵を取得し、メタ鍵を利用して、データ送受信ブロック161がコンテンツデータ3とともに受信した暗号化鍵（コンテンツデータ3用）を復号する。

【0211】暗号化処理サブブロック187は、復号して取得した暗号化鍵（コンテンツデータ3用）を利用して暗号化されているコンテンツデータ3を復号する。

【0212】ステップS124において、マイクロプロセッサ182は、復号処理が必要なコンテンツデータ単位以外に、デジタル署名の検証が必要なデータ単位がコントローラ162から転送されていることを認識する。

【0213】マイクロプロセッサ182がコンテンツデータ3の復号処理を実行していない場合（マイクロプロセッサ182が、図6のタイム1-2の状態である場合）、ステップS125において、マイクロプロセッサ182は、デジタル署名の検証に要する時間を算出する。

【0214】始めに、マイクロプロセッサ182は、コンテンツデータ3のデータ単位を復号する場合に要する時間を算出する。マイクロプロセッサ182は、メタデータ3のフィールド4の記述から、データ再生装置152が、コンテンツデータ3を出力するために、暗号化処理ブロック163に対して要求するコンテンツデータ3の復号処理結果の転送速度は2Mbpsであると認識する。そこで、マイクロプロセッサ182は、DESのアルゴリズムで暗号化されているコンテンツデータを復号する自分自身の能力は4Mbpsであるため、データ再生装置152が要求するデータ単位を処理するためには0.5秒の時間が必要であると算出する（図6のタイム1-1、タイム2-1、タイムn-1は0.5秒となる）。

【0215】次に、マイクロプロセッサ182は、デジタル署名の検証に要する時間を算出する。マイクロプロセッサ182は、DSAのアルゴリズムで生成されているデジタル署名を検証する自分自身の能力は1Mbpsであるため、データ再生装置152が要求するデータを処

理するためには2秒の時間が必要であると算出する。

【0216】ステップS126において、マイクロプロセッサ182が、ステップS125で算出した結果が判断される。マイクロプロセッサ182は、ステップS125で算出した時間から、次の復号処理が必要なコンテンツデータ3のデータ単位（図6の最優先処理データ単位2）が、コントローラ162から転送されてくるまでの間（図6のタイム1-2、タイム2-2）に、デジタル署名を検証することは不可能と認識する。

【0217】ステップS127において、マイクロプロセッサ182は、デジタル署名の検証をどのように処理するか判断するため、メタデータ3のフィールド6に記述されている取扱情報を確認する。

【0218】ステップS128において、マイクロプロセッサ182は、メタデータ3のフィールド6には、デジタル署名の検証の取扱方法として、コントローラ162に対する通知、およびデジタル署名の検証の遅延処理が設定されていると認識する。そこで、マイクロプロセッサ182は、コントローラ182に対してデジタル署名の検証を、最優先処理であるコンテンツデータ3の全てのデータ単位の復号処理が終了した後に処理することを通知するとともに、デジタル署名の検証を必要とするデータ単位をフラッシュメモリ185に記憶する。

【0219】ステップS129において、マイクロプロセッサ182は、復号処理が必要なコンテンツデータ3のデータ単位を全て復号処理したか否かを判定し、復号処理が全て終了したと判定するまで、復号処理を優先して処理する。

【0220】ステップS129において、マイクロプロセッサ182は、復号処理が必要なコンテンツデータ3のデータ単位を全て復号処理したと判定した場合、処理は、ステップS130に進む。

【0221】ステップS130において、マイクロプロセッサ182は、フラッシュメモリ185に記憶させておいたデジタル署名の検証が必要なデータの処理を行う（図6の遅延処理データを処理する）。

【0222】ステップS132において、マイクロプロセッサ182は、デジタル署名の検証を全て終了したと判定した場合、処理を終了する。

【0223】次に、STB151が、メタデータ4およびコンテンツデータ4を受信して処理する場合について説明する。

【0224】ステップS111乃至ステップS127の処理は上述したメタデータ3およびコンテンツデータ3を受信した場合と同様の処理である。

【0225】ステップS128において、マイクロプロセッサ182は、メタデータ4のフィールド6には、デジタル署名の検証の取扱方法として、デジタル署名の検証が必要なデータが転送されてきた場合であって

も、そのデータを無視すると設定されていると認識し、最優先処理であるコンテンツデータ4の復号を続ける。

【0226】その後、マイクロプロセッサ182は、コンテンツデータ4の復号が全て終了したと判定した場合、全ての処理を終了する。

【0227】ここでは、遅延処理するデジタル署名の検証が必要なデータを、最優先処理が終了するまでフラッシュメモリ185に記憶させることとしたが、記憶先なども、メタデータに設定することが可能である。また、コントローラ162がデジタル署名の検証を必要とするデータの転送を中止するように予め設定しても良い。

【0228】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータや、STB151などに、記録媒体からインストールされる。

【0229】図27は、一連の処理を実行するソフトウェアがインストールされるパーソナルコンピュータ201の構成例を示している。パーソナルコンピュータ201は、CPU(Central Processing Unit)211を内蔵している。CPU211にはバス214を介して、入出力インタフェース215が接続されている。入出力インタフェース215には、キーボード、マウスなどの入力デバイスよりなる入力部216、処理結果としての例えば音声信号を出力する出力部217、処理結果としての画像を表示するディスプレイなどよりなる表示部218、プログラムや各種データを格納するハードディスクドライブなどよりなる記憶部219、LAN(Local Area Network)やインターネットを介してデータを通信するモデムなどよりなる通信部220、および、磁気ディスク222(フロッピーディスクを含む)、光ディスク223(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク224(MD(Mini Disc)を含む)、もしくは半導体メモリ225などの記録媒体に対してデータを読み書きするドライブ221が接続されている。バス214には、ROM(Read Only Memory)212およびRAM213が接続されている。

【0230】一連の処理を実行するソフトウェアは、磁気ディスク222、光ディスク223、光磁気ディスク224、および半導体メモリ225に格納された状態でパーソナルコンピュータ201に供給され、ドライブ221によって読み出されて、記憶部219に内蔵されるハードディスクドライブにインストールされる。記憶部219にインストールされているエージェントプログラムは、入力部216に入力されるユーザからのコマンド

に対応するCPU211の指令によって、記憶部219からRAM213にロードされて実行される。

【0231】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0232】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0233】

【発明の効果】以上のように、本発明の情報処理装置、情報処理方法、および記録媒体のプログラムによれば、コンテンツデータの特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識し、処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理するようにしたので、低コストで、かつ、機能変更が容易な、迅速にデータを処理することができるシステムを実現することが可能になる。

【図面の簡単な説明】

【図1】従来の復号LSIの構成例を示すブロック図である。

【図2】本発明を適用したデータ処理システムの構成例を示すブロック図である。

【図3】データ送信装置の処理を説明するフローチャートである。

【図4】データ受信装置の処理を説明するフローチャートである。

【図5】データ受信装置の処理を説明する図3の続きのフローチャートである。

【図6】復号処理部に転送されてくるデータ単位を説明する図である。

【図7】本発明を適用したコンテンツ配信システムの概念を示す図である。

【図8】コンテンツサーバの構成例を示すブロック図である。

【図9】データ暗号化装置の詳細な構成例を示すブロック図である。

【図10】サービスサーバの構成例を示すブロック図である。

【図11】決済サーバの構成例を示すブロック図である。

【図12】利用者端末の構成例を示すブロック図である。

【図13】セットトップボックスの構成例を示すブロック図である。

【図14】暗号化処理ブロックの詳細な構成例を示すブロック図である。

【図15】暗号化処理ブロックが送受信するデータ形式

の例を示す図である

【図16】コンテンツサーバの処理を説明するフローチャートである。

【図17】コンテンツサーバが生成するメタデータの例を示す図である。

【図18】コンテンツサーバが送信するデータのフォーマットの例を示す図である。

【図19】サービスプロバイダの処理を説明するフローチャートである。

【図20】サービスサーバが生成するメタデータの例を示す図である。

【図21】決済サーバの使用権情報の発行処理を説明するフローチャートである。

【図22】決済サーバの使用権情報の発行処理を説明する図19の続きのフローチャートである。

【図23】使用権情報の例を示す図である。

【図24】セットトップボックスの処理を説明するフローチャートである。

【図25】セットトップボックスの処理を説明する図22の続きのフローチャートである。

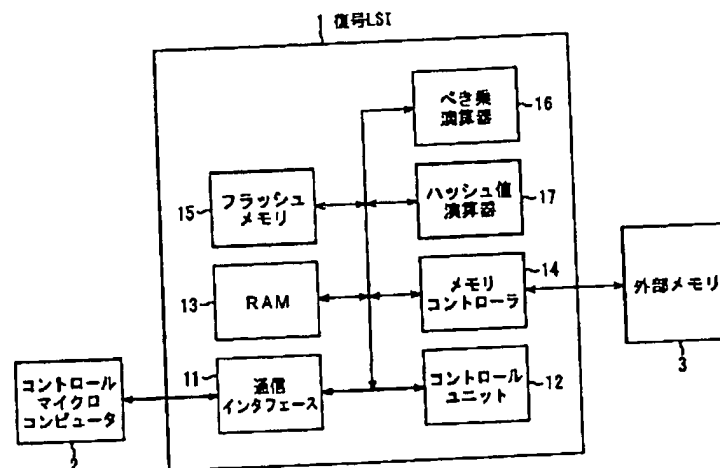
【図26】セットトップボックスの処理を説明する図23の続きのフローチャートである。

【図27】パーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

21 データ送信装置、 22 ネットワーク、 23 データ受信装置、 41 データ受信部、 42 データ処理判断部、 43 復号処理部、 44 計算部、 45 データ記憶部、 56 利用者端末、 151 セットトップボックス、 152 データ再生装置、 161 データ送受信ブロック、 162 コントローラ、 163 暗号化処理ブロック、 164 フラッシュメモリ、 165 外部RAM、 181 入出力インタフェースブロック、 182 マイクロプロセッサ、 183 RAM、 184 乱数生成ブロック、 185 フラッシュメモリ、 186 暗号化処理部、 187 暗号化処理サブブロック、 188 デジタル署名検証サブブロック、 189 ハッシュ値計算サブブロック

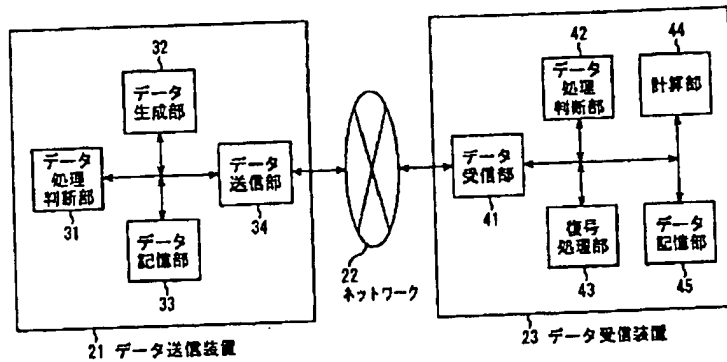
【図1】



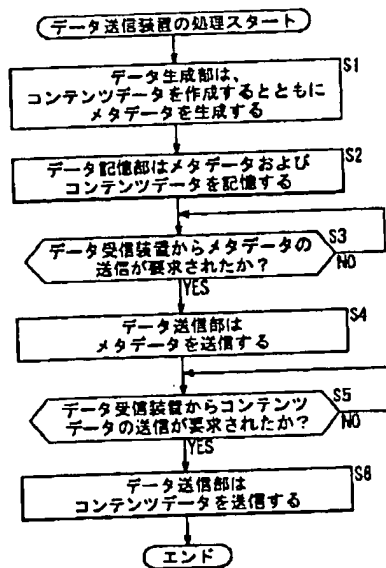
【図15】

フィールド1	フィールド2	フィールド3	フィールド4
データ種識別フィールド	データ番号フィールド	データ長フィールド	データフィールド

【図2】

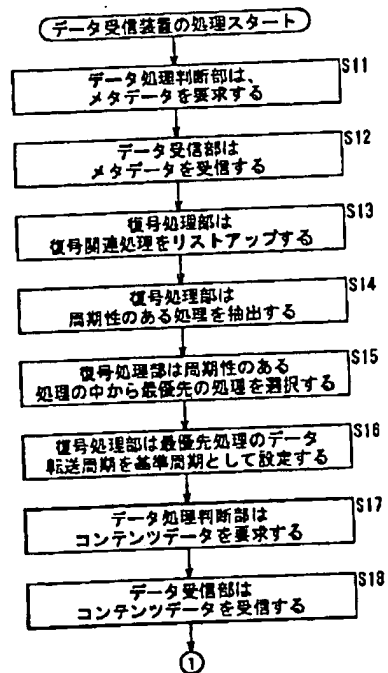


【図3】



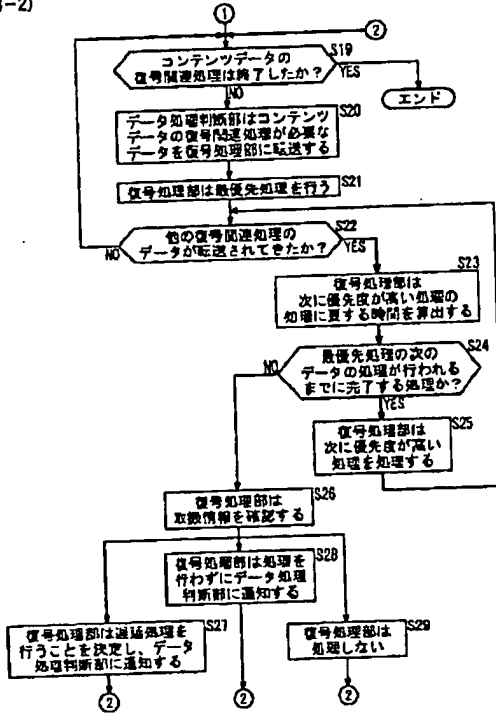
【図4】

(4-1)

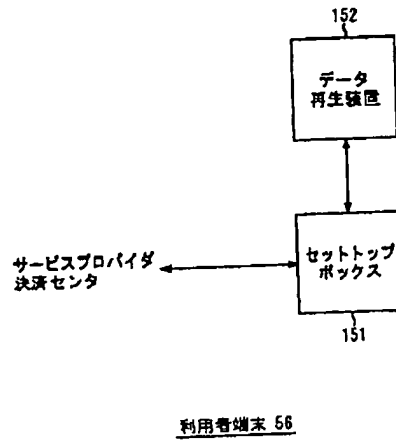


【図5】

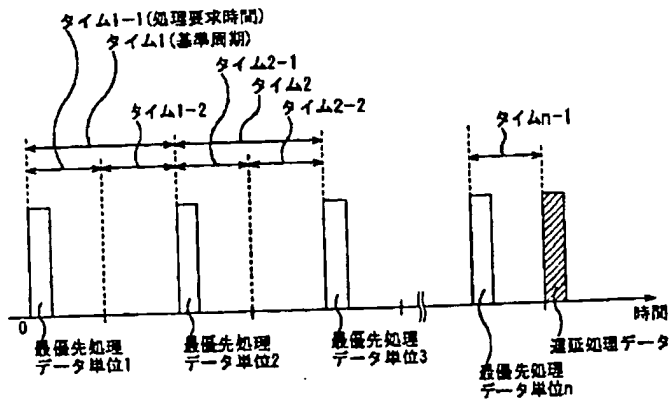
(4-2)



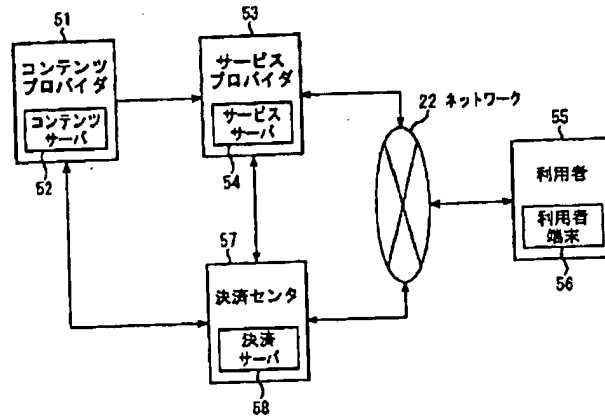
【図12】



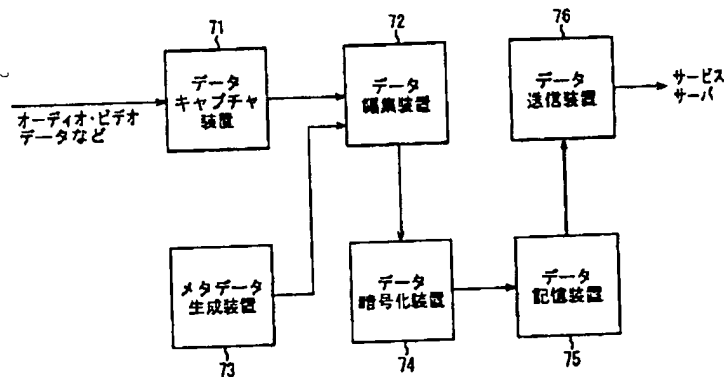
【図6】



【図7】



【図8】



コンテンツサーバ 52

【図17】

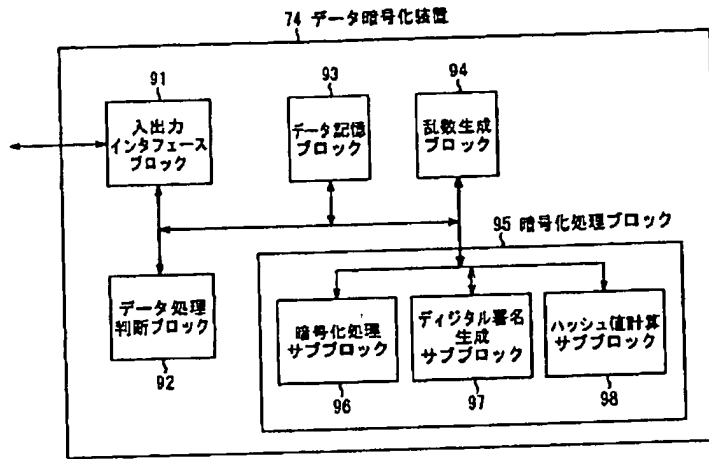
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
コンテンツプロバイダID コンテンツID 権利発生日時	1 ストリーミング 2 買い取り 3 配信形式1年	1 1000 2 1000 3 1000	再生時間 10分 総データ量 150MB データ形式 MP4 転送速度 28000	デジタル番号 DGA 番号 DCS データ単位 25GB	転送速度 優先度 転送 番号 1000 2 通知 (DGA) 1000 1 通知 (DCS) 1000 1 通知

(A) メタデータ1

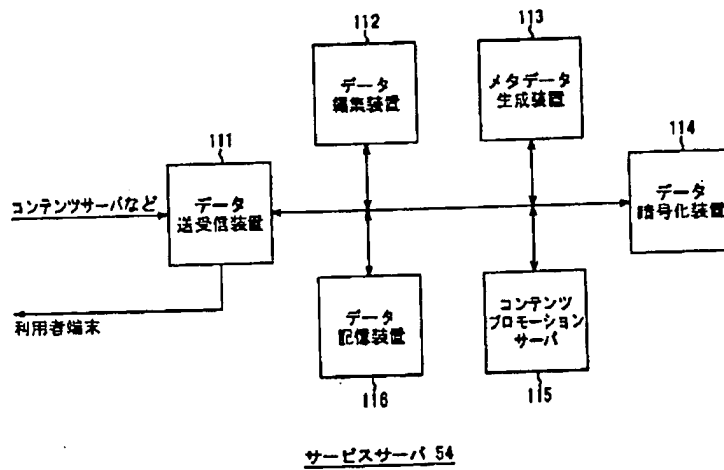
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
コンテンツプロバイダID コンテンツID 権利発生日時	1 ストリーミング 2 買い取り 3 配信形式1年	1 1000 2 1000 3 1000	再生時間 10分 総データ量 150MB データ形式 MP4 転送速度 28000	デジタル番号 DGA 番号 DCS データ単位 25GB	転送速度 優先度 転送 番号 1000 2 通知 (DGA) 1000 1 通知 (DCS) 1000 1 通知

(B) メタデータ2

【図9】



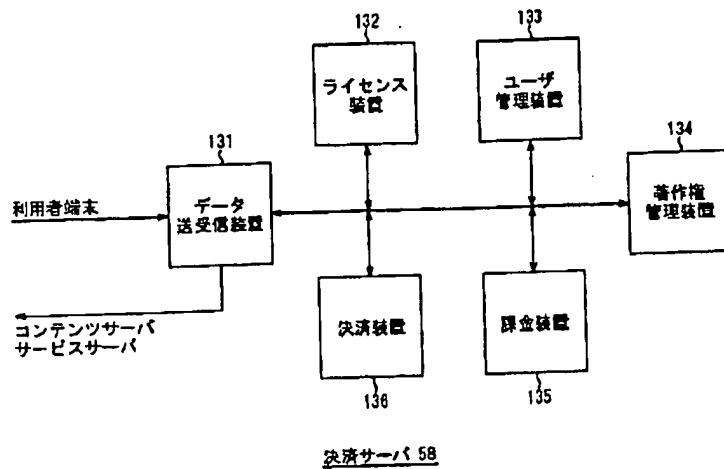
【図10】



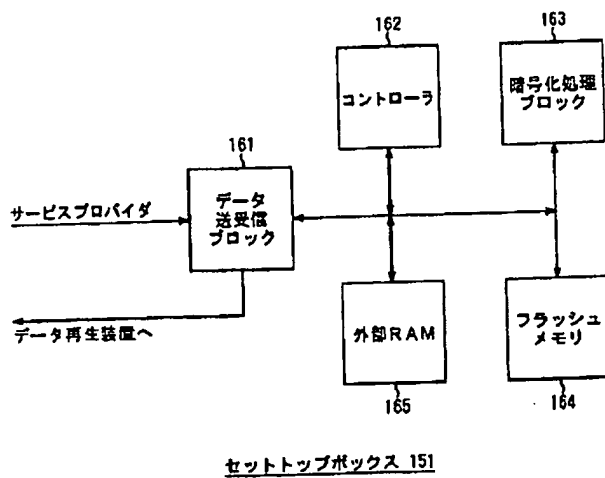
【図23】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID コンテンツID 権利発生日時	2 1 2000年 1月2日	1 ストリーミング 1 *30	メタ鍵	デジタル署名

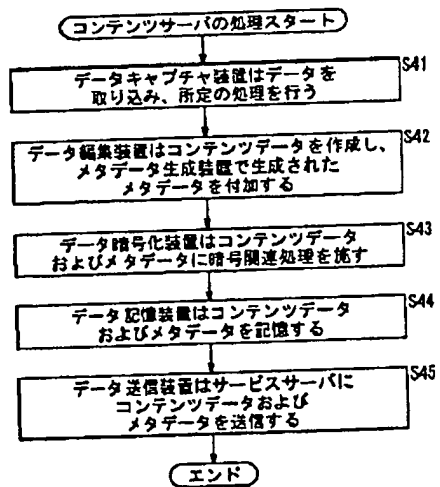
【図11】



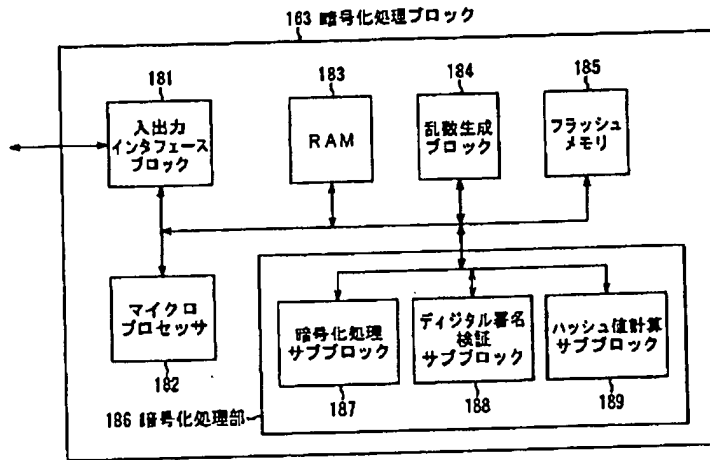
【図13】



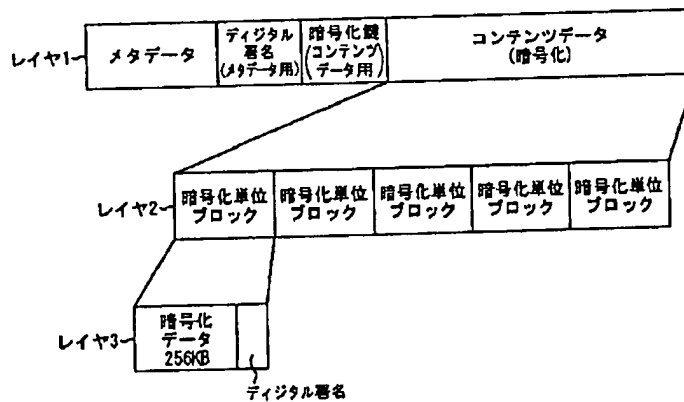
【図16】



【図14】



【図18】



【図20】

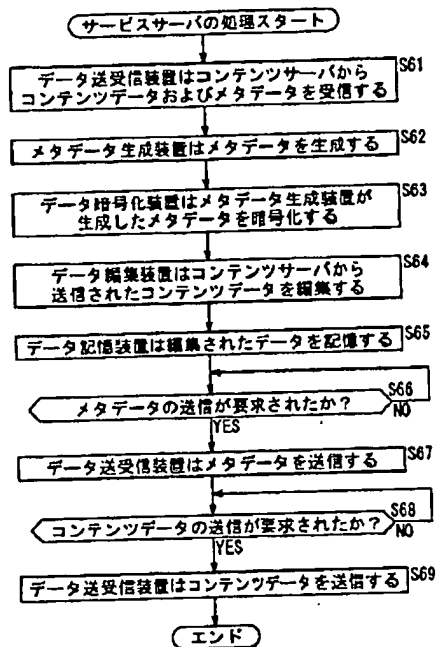
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
サービスプロバイダID コンテンツID メタデータ作成日時	1 ストリーミング 2 買い取り 3 配信形式	1 K30 2 H150 3 K60	再生時間 総データ量 データ形式 転送速度	デジタル署名 暗号化 データ単位	署名検証 (DSA) 署名 (DES)
2000年 1月2日	2000年 1月2日	2000年 1月2日	10分 150MB MP3 2Mbps	DSA DES 256KB	署名検証 (DSA) 署名 (DES)

(A) メタデータ3

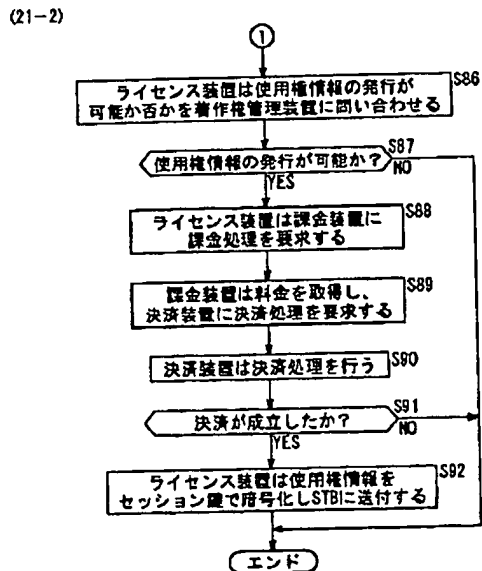
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
サービスプロバイダID コンテンツID メタデータ作成日時	1 ストリーミング 2 買い取り 3 配信形式	1 K30 2 H150 3 K60	再生時間 総データ量 データ形式 転送速度	デジタル署名 暗号化 データ単位	署名検証 (DSA) 署名 (DES)
2000年 1月2日	2000年 1月2日	2000年 1月2日	10分 150MB MP3 2Mbps	DSA DES 256KB	署名検証 (DSA) 署名 (DES)

(B) メタデータ4

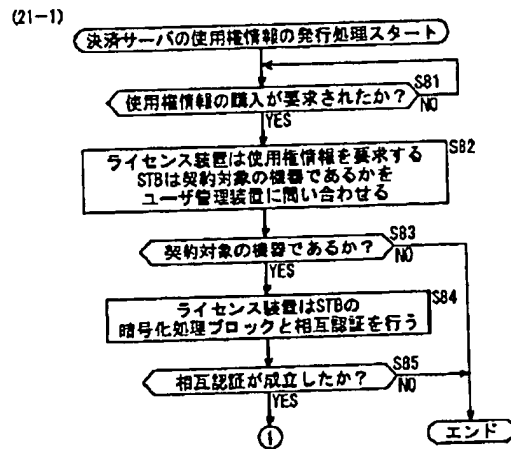
【図19】



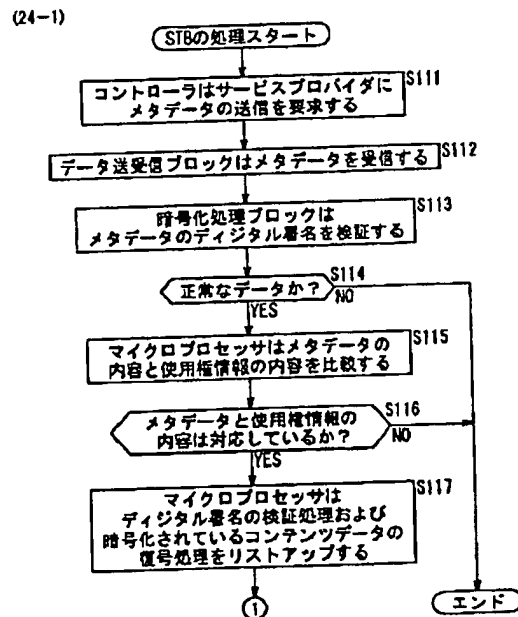
【図22】



【図21】

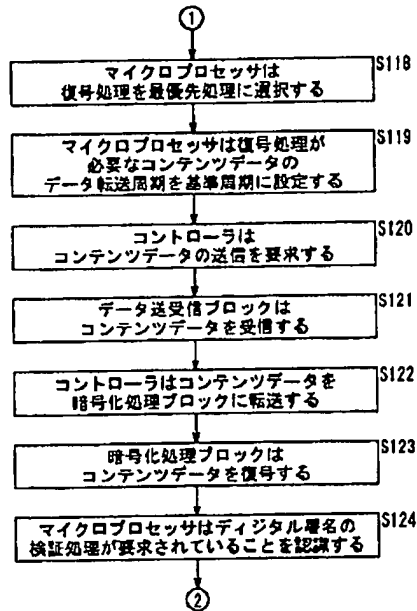


【図24】



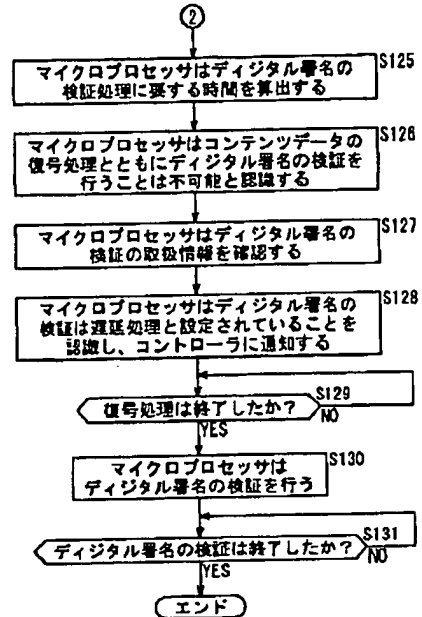
【図25】

(24-2)

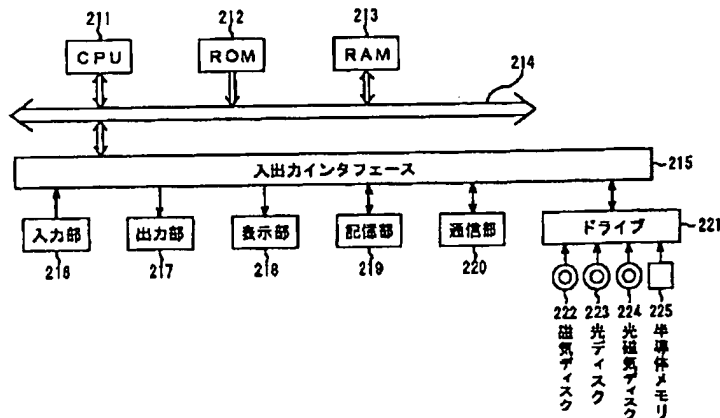


【図26】

(24-3)



【図27】



パーソナルコンピュータ 201